Homeworks: Algorithms on Elliptic Curves

2024/25

There will be four homework assignments for which a maximum of 40 points can be obtained in total. A minimum of 25 points is required for credit.

All steps should be explained in detail (preferably by references to assertions, examples, or exercises).

1. Homework

To be submitted till 26th March, 2 pm

1.1. Find a short WEP which is $\mathbb{F}_3$-equivalent to the WEP

$$w = y^2 + y(2x + 1) - (x^3 + 2x^2 + 2x) \in \mathbb{F}_3[x, y].$$

5 points

1.2. Decide whether the WEP is $y^2 - (x^3 + 4x^2 - x - 4) \in K[x, y]$ is smooth if (a) $K = \mathbb{Q}$, (b) $K = \mathbb{F}_5$.

5 points

2. Homework

To be submitted till 30th April, 2 pm

2.1. Find all elements and draw the tables of the group operations $\ominus$, $\oplus$ of the group of the elliptic curve C given by the WEP $w = y^2 - (x^3 + x) \in \mathbb{F}_5[x, y]$.

4 points

2.2. Decide whether the WEP $y^2 - (x^3 + 3x - 1) \in \mathbb{F}_7[x, y]$ is $\mathbb{F}_7$-equivalent to some Montgomery polynomial.

3 points

2.3. Depending on the binary length $k = l_2(n)$ and the number of inversions, multiplications and squarings (I, M, S) in a field $\mathbb{F}$, estimate the time complexity of computing the power $[n]P$ of an element P of the Montgomery curve using the Montgomery's ladder.

3 points